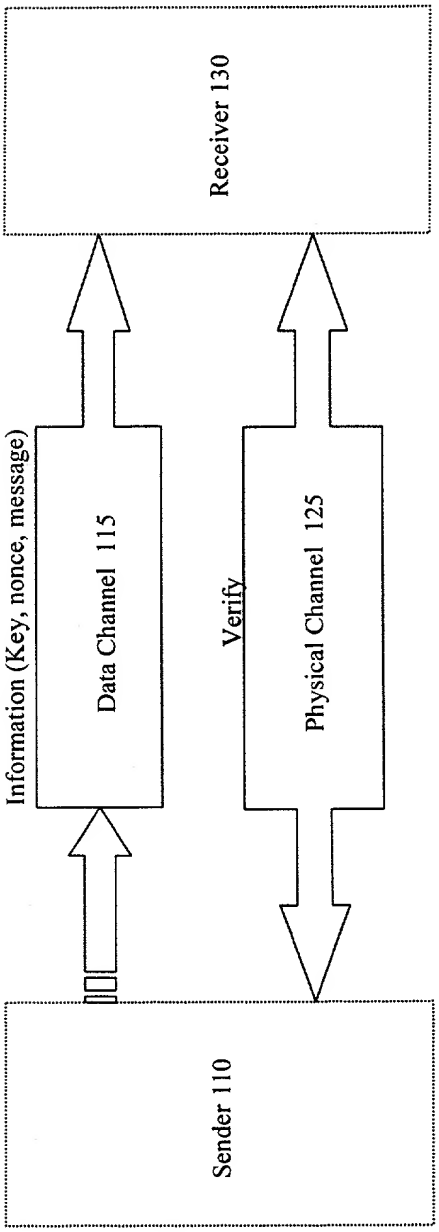
100
Receiver 130
Information (Key, nonce, message)
Data Channel 115
Verify
Physical Channel 125
Sender 110

FIG. 1

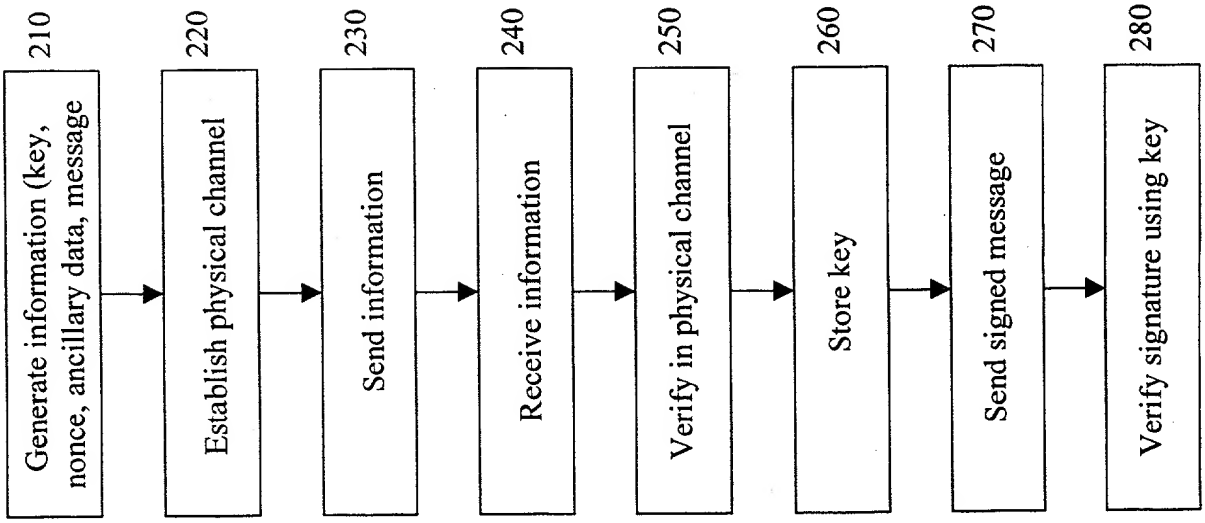
210
Generate information (key, nonce, ancillary data, message
220
Establish physical channel
230
Send information
240
Receive information
250
Verify in physical channel
260
Store key
270
Send signed message
280
Verify signature using key

FIG. 2

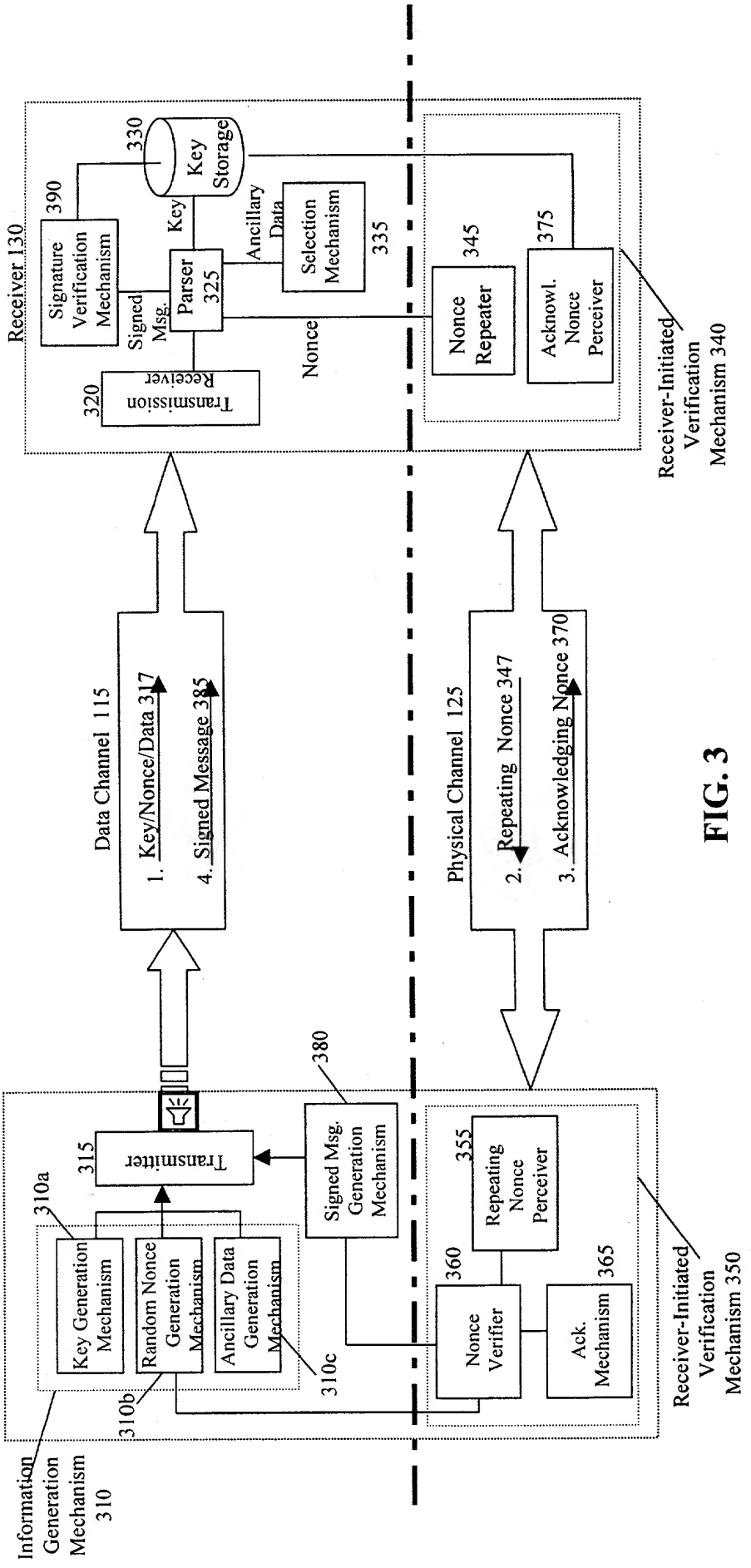
Receiver 130
Signature Verification Mechanism
390
Signed Msg.
Parser 325
Key
Key Storage
330
Ancillary Data
Selection Mechanism
335
Nonce
Transmission Receiver
320
Nonce Repeater
345
Acknowl. Nonce Perceiver
375
Receiver-Initiated Verification Mechanism 340
Data Channel 115
1. Key/Nonce/Data 317
4. Signed Message 385
Physical Channel 125
2. Repeating Nonce 347
3. Acknowledging Nonce 370
Sender 110
310a
Key Generation Mechanism
Random Nonce Generation Mechanism
Ancillary Data Generation Mechanism
310b
310c
Transmitter
315
Signed Msg. Generation Mechanism
380
Repeating Nonce Perceiver
355
Nonce Verifier
360
Ack. Mechanism
365
Receiver-Initiated Verification Mechanism 350
Information Generation Mechanism 310

FIG. 3

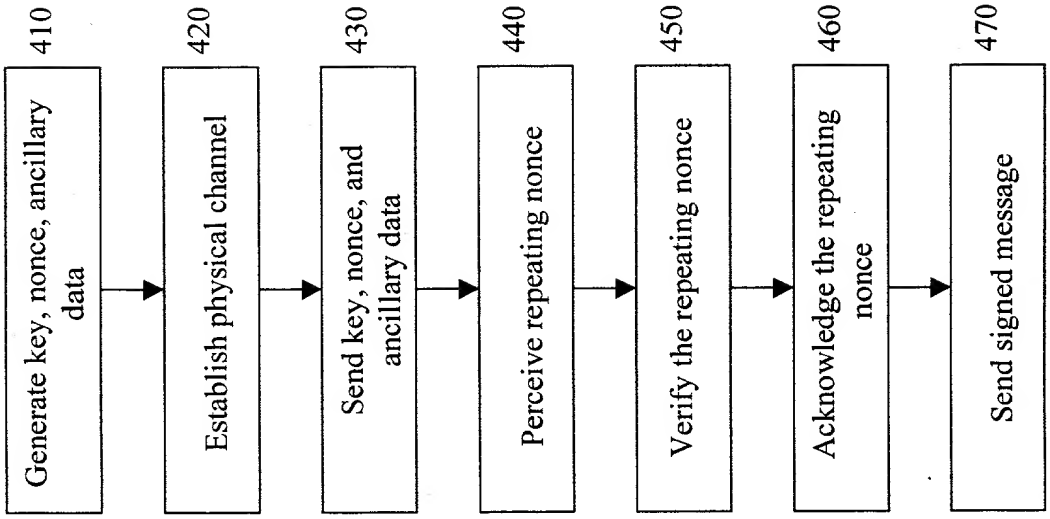
410
Generate key, nonce, ancillary data
420
Establish physical channel
430
Send key, nonce, and ancillary data
440
Perceive repeating nonce
450
Verify the repeating nonce
460
Acknowledge the repeating nonce
470
Send signed message

FIG. 4

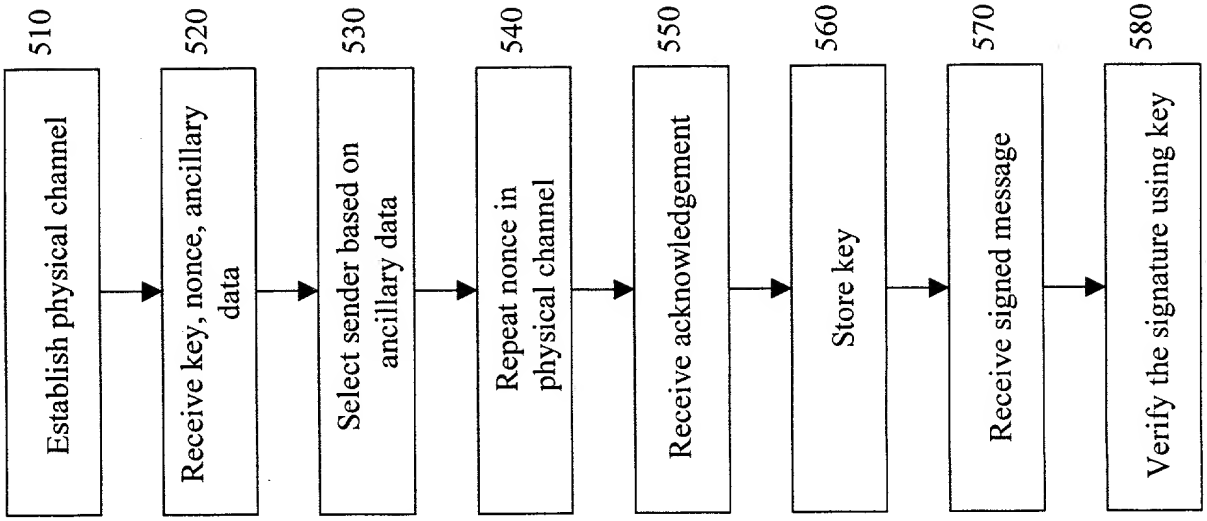
510
Establish physical channel
520
Receive key, nonce, ancillary data
530
Select sender based on ancillary data
540
Repeat nonce in physical channel
550
Receive acknowledgement
560
Store key
570
Receive signed message
580
Verify the signature using key

FIG. 5

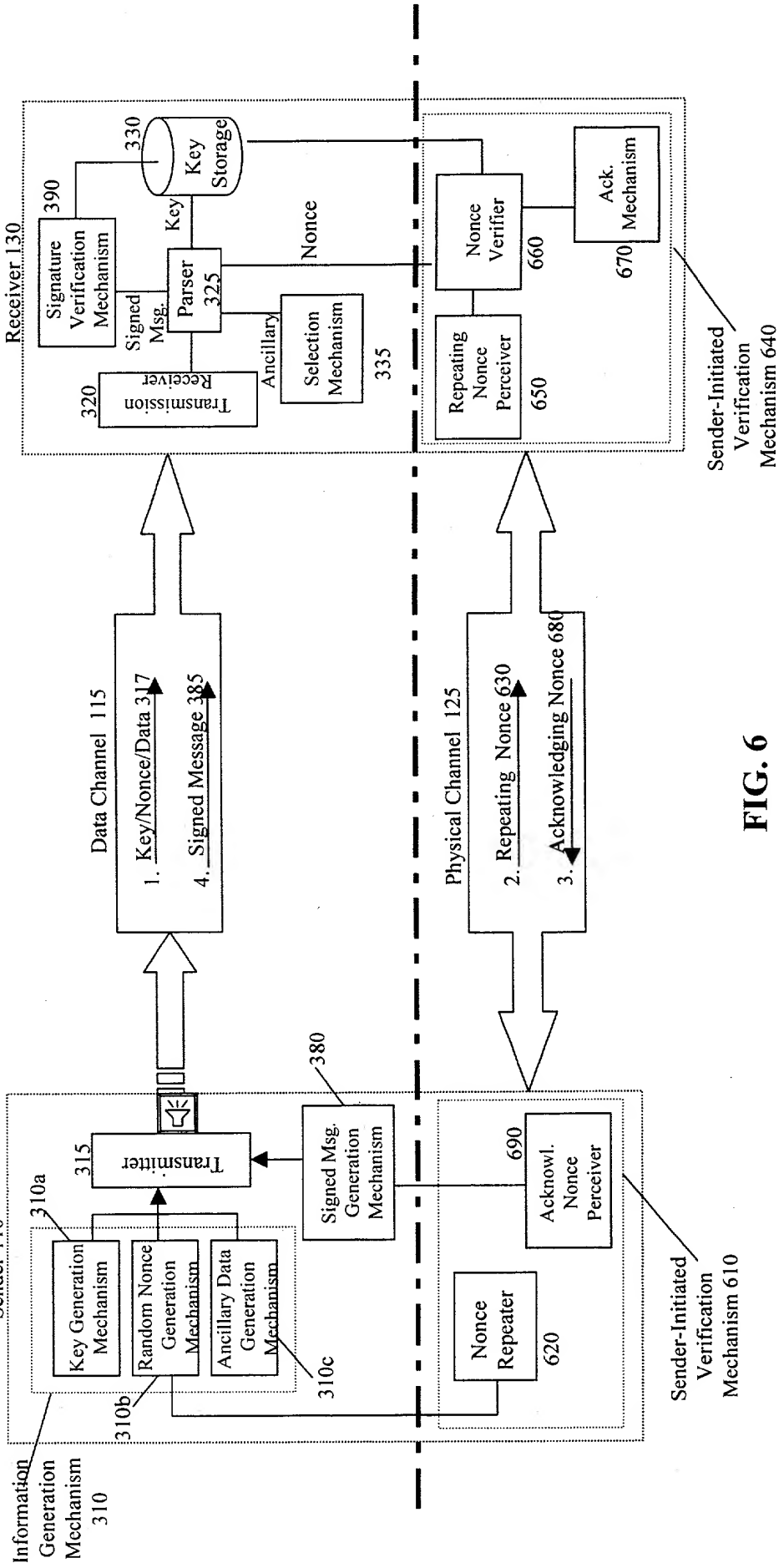
Receiver 130
Signature Verification Mechanism
390
Key Storage
330
Key
Nonce
Signed Msg.
Parser 325
Ancillary
Selection Mechanism
335
Transmission Receiver
320
Nonce Verifier
660
Ack. Mechanism
670
Repeating Nonce Perceiver
650
Sender-Initiated Verification Mechanism 640
Data Channel 115
1. Key/Nonce/Data 317
4. Signed Message 385
Physical Channel 125
2. Repeating Nonce 630
3. Acknowledging Nonce 680
380
Signed Msg. Generation Mechanism
Transmitter
315
690
Acknowl. Nonce Perceiver
Sender 110
310a
Key Generation Mechanism
Random Nonce Generation Mechanism
Ancillary Data Generation Mechanism
310c
310b
Nonce Repeater
620
Sender-Initiated Verification Mechanism 610
Information Generation Mechanism 310

FIG. 6

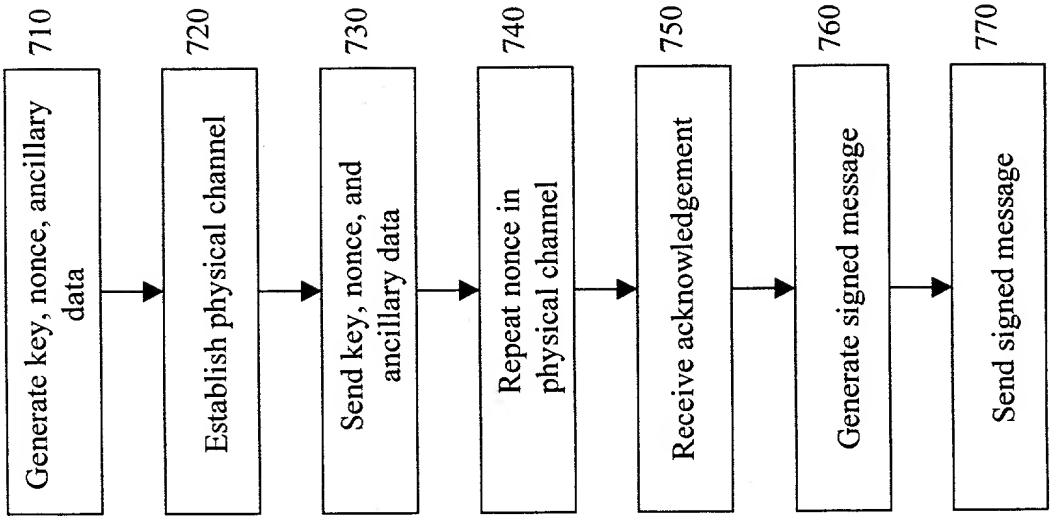
710
Generate key, nonce, ancillary data
720
Establish physical channel
730
Send key, nonce, and ancillary data
740
Repeat nonce in physical channel
750
Receive acknowledgement
760
Generate signed message
770
Send signed message

FIG. 7

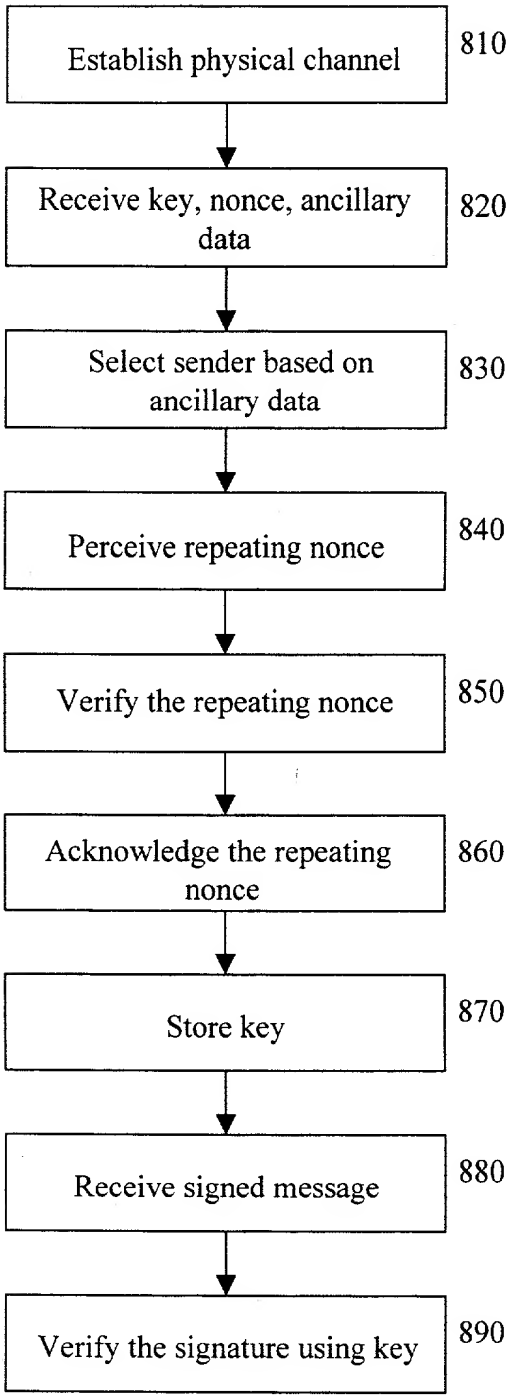
Establish physical channel
810
Receive key, nonce, ancillary data
820
Select sender based on ancillary data
830
Perceive repeating nonce
840
Verify the repeating nonce
850
Acknowledge the repeating nonce
860
Store key
870
Receive signed message
880
Verify the signature using key
890

FIG. 8